UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,415	11/15/2001	Frank Muller	PTT-124 (402562US)	9606

7265   7590   08/04/2005

MICHAELSON AND WALLACE
PARKWAY 109 OFFICE CENTER
328 NEWMAN SPRINGS RD
P O BOX 8489
RED BANK, NJ 07701

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/937,415	MULLER ET AL.
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _09 June 2005_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _18-26_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _18-26_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _15 November 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 17 have been presented for examination. Claims 1 – 17 have

been canceled; and new claims 18 – 26 have been added in an amendment filed

6/9/2005. Therefore, presently pending claims are 18 – 26.

Response to Arguments

1.   Applicant's arguments filed on 6/9/2005 with respect to the subject matter

of the instant existing claims have been fully considered but are not persuasive.

Because all of the previous claims 1 – 17 have been cancelled, see the same

reasons set forth in the following Office action in rejecting the new claims 18 –

26.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of
making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
set forth the best mode contemplated by the inventor of carrying out his invention.

2.   Claim 18 is rejected under 35 U.S.C. 112, first paragraph, as failing to

comply with the enablement requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to enable one

skilled in the art to which it pertains, or with which it is most nearly connected, to

make and/or use the invention.

This is because a typical embodiment of any authentication system would

include both enciphering and deciphering sections. However, the deciphering

mechanism is not clearly and specifically addressed in the specification – For

example, Applicant remarks "the receiver of the enciphered section that is either

the same or complementary to the enciphering section present at the sending

location ... those of skill fully understand that the deciphering section employs

the same inventive methodology though in the same or an opposite manner

(Page 22)". Examiner notes (a) the mechanism of deciphering functions,

especially as identified by Applicant to be "complementary to the enciphering

section present at the sending location or using the same inventive methodology

though in an opposite manner" is not clearly and specifically addressed in the

specification; (b) the corresponding example of deciphering procedure to the

enciphering function as shown in TABLE I (Page 4) is respectively requested by

Examiner to demonstrate the deciphering procedure from step 0 to step 9. With

these clarifications, one skilled in the art clearly can further assure using the

claimed invention to complete the entire process of the transmitted and received

message for authentication purpose.

Any other claims not addressed are rejected by virtue of their dependency

should also be corrected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102

that forms the basis for the rejections under this section made in this Office

action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claims 18 – 26 are rejected under 35 U.S.C. 102(b) as being anticipated

by Ritter (Patent Number: 4979832), hereinafter referred to as Ritter.

As per claim 18, Ritter teaches a method for authentication of a string of a

computer readable medium containing computer executable instructions which,

when executed, authenticate a string having a plurality of input characters

through use of a method which relies on an enciphering function that enciphers,

in response to a string of key characters, the string of; input characters to yield a

corresponding string having a plurality of output enciphered characters, the

method comprising the steps of:

modifying said enciphering function, by application of a modification

function and in response to a string of modification characters (Ritter: see for

example, Figure 1 Element 18 & 20, Column 5 Line 50 – 53 and Column 6 Line

17 – 20: The CHANGES CONTROLLER as taught by Ritter is qualified to

perform the modification function); and

enciphering, by application of the enciphering function and in response to said string of key characters, said string of input characters so as to yield the corresponding string of output enciphered characters (Ritter: see for example, Figure 1 Element 12, 14 & 16, Column 5 Line 50 – 53 and Column 6 Line 8 – 16: The COMBINER / SUBSTITUTE as taught by Ritter is to perform the enciphering function and Pseudo-Random number can serve as a KEY); wherein:

said modification function is applied initially to said enciphering function, that is prior to (Ritter: Figure 1 Element 20 & 12) the application of the enciphering function to generate all of the enciphered characters in the corresponding string of output enciphered characters (Ritter: see for example, Figure 1 Element 18 & 20 and Column 6 Line 21 – 24); and

said modification function, once so initially applied, modifies the enciphering function (Ritter: Figure 1 Element 10 & 18 and Column 6 Line 17 – 24) in response to the modification characters (Ritter: Figure 1 Element 20), the modification characters being derived from said string of input characters (Ritter: see for example, (Ritter: Figure 1 Element 10).

As per claim 19, Ritter teaches the modification characters are also derived from said string of key characters (Ritter: see for example, Figure 1 Element 16, Column 5 Line 50 – 53 and Column 6 Line 8 – 16).

As per claim 20 and 26, Ritter teaches the modification function replaces a character of the string of modification characters by a replacement character

obtained by addition of two or more characters of the string of modification

characters modulo the number of possible different characters in each of the

modification characters (Ritter: see for example, Column 2 Line 16 – 18, Column

2 Line 23 – 25 and Column 11 Line 1 – 4: Examiner notes since the replacement

character resulted from the combination / addition of two or more different

characters must be coming from the predefined set of characters (i.e., S-Box or

the substitution table), the modulo of addition with the size of S-Box or the

substitution table must be utilized accordingly).

As per claim 21, Ritter teaches the modification function modifies

sequence numbers of two or more of the characters of the string of modification

characters (Ritter: see for example, Figure 1 Element 10 &16, Column 6 Line 20

– 24 and Column 11 Line 7 – 12).

As per claim 22, Ritter teaches the modification function comprises, as an

initial function, a function which was previously used for determining an earlier

string of the output enciphered characters than the corresponding string of the

output enciphered characters (Ritter: see for example, Figure 1 Element 18 & 20

and 12 & 14 and Column 6 Line 21 – 24).

As per claim 23, Ritter teaches the enciphering function comprises a

substitution function (Ritter: see for example, Column 6 Line 20 – 24).

As per claim 24, Ritter teaches the enciphering function comprises a non-invertible function (Ritter: see for example, Abstract 4th Paragraph Line 4 – 5).

As per claim 25, Ritter teaches the enciphering function comprises a substitution box having replacement characters for characters of the string of input characters, and the modification function exchanges, based on the string of modification characters, two or more characters of the substitution box (Ritter: see for example, Figure 1 and Column 6 Line 1 – 35: The "operation on a single block of data" as taught by Ritter is qualified as the S-Box).

Conclusion

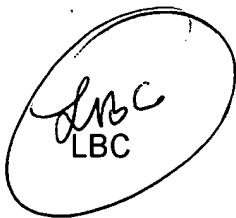**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100